Security Quickie 2-27-02: E-mail Scam$

You can get a message to practically anyone in the world in a few moments, just by using e-mail. Your aunt in Panama Beach, Florida, your business associate in Kyoto, Japan, your child's 'pen-pal' in Maputo, Mozambique, or your co-worker just down the hall: almost anyone can be easily reached by e-mail. This also means that practically anyone can reach you via e-mail, too, and this unfortunately includes scam artists, identity thieves, hoax creators, and other not-so-nice people.

E-mail scams have recently been entering State e-mail systems. Be wary of any pleas for financial aid, investment opportunities, or attempts to "get to know you better" by unknown sources. Many scams promise you (whoever the recipient might be) millions of dollars if you just help transfer money out of 'X' country, or offer the potential for vast earnings (like pyramid schemes), or even just claim you'll get a 'good feeling' inside because you helped a stranger in need. The vast majority of these types of e-mails are scams. The senders want one thing – your money – and will play on your fears, desires, greed, or confusion to get confidential financial or personal information from you.

Never send out confidential information to someone you don't know. If you receive a request for information, or a request to confirm confidential information via e-mail, be extremely cautious and doubtful as to the validity of the message. Neither government agencies nor businesses should request this type of information via unencrypted e-mail, and if they do, give the business or agency a call and confirm the request (and complain about the poor security issue). As a rule, never put confidential information into an unencrypted e-mail and don't give out personal information to people you do not know. Social Security numbers, bank account information, credit card accounts numbers, business accounts, and any other private, confidential, or personal information should not be shared with unknown sources. (Or even known sources that don't need it!)

The Information Security Office has put together a brief description of recently seen **e-mail scams**. To view this information: contact William.Hubbard@iowa.gov. If you think you might be the recipient of an e-mail scam, check out the listing. If you see the scam (or mass mailing) there, simply delete the e-mail message from your system. If you have received a new scam or are unsure about the e-mail message you've received, forward it to the Security Alert account. We'll post new scams so other people can benefit from the knowledge. Being forewarned is a good start at protecting yourself from these scams, but being skeptical about fantastic 'opportunities' is even better. In the final consideration, it's only money. **Your** money…